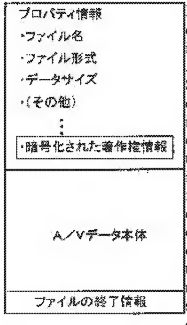
# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-015960**
(43)Date of publication of application : **17.01.2003**

(51)Int.Cl. **G06F 12/14**
**G06F 12/00**
**G11B 20/10**
**H04L 9/08**
**H04L 9/32**
**H04N 5/91**

(21)Application number : **2002-070374** (71)Applicant : **SONY CORP**
(22)Date of filing : **27.09.1996** (72)Inventor : **KORI TERUHIKO**

## (54) FILE GENERATION METHOD AND DATA PROCESSING METHOD




(57)Abstract:
PROBLEM TO BE SOLVED: To make an A/V data file handled on a computer contain copyright information, and to protect the copyright of the A/V data.
SOLUTION: The copyright information, that is composed of file copy generation management information and is encoded with a given encryption key kc, is stored in the header part of the file. When the file is accessed, the copyright information is extracted from the header part at first. If a user who has accessed has not the encryption key kc, the user can not decode the copyright information, and, accordingly, the user can not read the A/V data stored in the file. When the file is copied, the copy generation management information is rewritten and is again stored as the copyright information, and thus the copy generation can be restricted. By encoding the main body of the A/V data with another encryption key kd and by encoding the key kd together with the copyright information with the key kc, the copyright can be protected more reliably.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－15960
（P2003－15960A）
(43)公開日　平成15年1月17日(2003.1.17)

| (51)Int.Cl.⁷ | 識別記号 | Ｆｉ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　12/14 | ３２０ | Ｃ０６Ｆ　12/14 | ３２０Ｅ | ５Ｂ０１７ |
| | | | ３２０Ｂ | ５Ｂ０８２ |
| 12/00 | ５３７ | 12/00 | ｂ３７Ｈ | ５Ｃ０５３ |
| Ｇ１１Ｂ　20/10 | | Ｇ１１Ｂ　20/10 | Ｈ | ５Ｄ０４４ |
| Ｈ０４Ｌ　9/08 | | Ｈ０４Ｎ　5/91 | Ｐ | ５Ｊ１０４ |

審査請求 有　請求項の数６　ＯＬ　（全 14 頁）　最終頁に続く

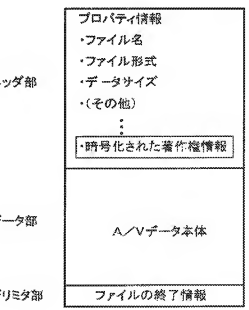
(21)出願番号　特願2002－70374(P2002－70374)
(62)分割の表示　特願平8－277130の分割
(22)出願日　平成８年９月27日(1996.9.27)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　部　順彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100087762
弁理士　杉浦　正知　（外１名）

最終頁に続く

(54)【発明の名称】　ファイル生成方法およびデータ処理方法

(57)【要約】
【課題】　コンピュータ上で扱われるＡ／Ｖデータファイルに対して著作権情報を持たせ、Ａ／Ｖデータの著作権を保護する。
【解決手段】　ファイルのコピーの世代制限情報からなり、所定の暗号化鍵ｋｃによって暗号化される著作権情報が、ファイルのヘッダ部に格納される。このファイルに対してアクセスした場合には、先ず、このヘッダ部から著作権情報が抽出される。アクセスを行なったユーザが暗号化鍵ｋｃを有していなければ著作権情報を復号化できないために、ファイルに格納されたＡ／Ｖデータを読み出すことができない。ファイルのコピーの際には、世代制限情報が書き換えられ再び著作権情報として格納されるため、コピーの世代を制限することができる。Ａ／Ｖデータ本体を別の暗号化鍵ｋｄで暗号化し、鍵ｋｄを著作権情報と共に鍵ｋｃで暗号化することによって、さらに確実に著作権保護を行なうことができる。



【特許請求の範囲】
【請求項1】 ディジタルデータの著作権情報を第1の暗号化鍵に基づき暗号化する第1の暗号化ステップと、上記ディジタルデータをデータファイルのデータ部に格納し、上記暗号化した著作権情報を上記データファイルの所定領域に格納してデータファイルを生成するステップとからなることを特徴とするファイル生成方法。
【請求項2】 請求項1に記載のファイル生成方法は、さらに、
上記ディジタルデータを第2の暗号化鍵で暗号化するステップを有し、上記著作権情報と共に上記第2の暗号化鍵を上記第1の暗号化鍵で暗号化し、上記データファイルの所定領域に格納することを特徴とするファイル生成方法。
【請求項3】 上記暗号化した著作権情報は、上記データファイルのヘッダ部に格納することを特徴とする請求項1に記載のファイル生成方法。
【請求項4】 ディジタルデータと、暗号化された該ディジタルデータの著作権情報とからなるデータファイルを受信するステップと、
上記暗号化されたディジタルデータの著作権情報を復号化し、著作権情報を抽出するステップと、
上記著作権情報に基づいて、上記ディジタルデータの取り扱いを制御するステップとからなることを特徴とするデータ処理方法。
【請求項5】 上記暗号化されたディジタルデータの著作権情報は、上記データファイルのヘッダ部に格納されていることを特徴とする請求項4に記載のデータ処理方法。
【請求項6】 第2の暗号化鍵で暗号化されたディジタルデータと、第1の暗号化鍵で暗号化された該ディジタルデータの著作権情報及び上記第2の暗号化鍵とからなるデータファイルを受信するステップと、
上記暗号化されたディジタルデータの著作権情報及び暗号化された第2の暗号化鍵を、第1の暗号化鍵で復号し、著作権情報及び第2の暗号化鍵を抽出するステップと、
上記暗号化されたディジタルデータを、上記抽出した第2の暗号化鍵で復号するステップとからなることを特徴とするデータ処理方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】この発明は、データファイルの属性情報として著作権情報を持たせ、この著作権情報を所定の方法に基づき暗号化することで、著作物として作成されたディジタルデータの著作権を保護するようなファイル生成方法およびデータ処理方法に関する。
【0002】
【従来の技術】近年、コンピュータの高速化やディジタル記録媒体の大容量化、コンピュータネットワークの発達、また、画像圧縮技術の発達などが目ざましい。それに伴い、ディジタル化された映像信号や音声信号、あるいはコンピュータによって作成されたCG(Computer Graphics)作品などがA/V(Audio/Video)データファイルとして記録されることが行なわれている。こうして記録されたA/Vデータファイルは、CD-ROMなどに複製され、あるいはネットワークを介して販売ならびに配布される。
【0003】このA/Vデータファイルは、例えばパーソナルコンピュータによって扱われる。そして、ユーザは、このパーソナルコンピュータに接続されたディスプレイ装置やオーディオ装置によってこのA/Vデータファイルを再生して楽しむことができる。
【0004】
【発明が解決しようとする課題】ところで、従来でも、所謂A/V機器において、ディジタル化された映像信号や音声信号が記録された記録媒体が販売されていた。A/V機器においては、例えば再生のみ、あるいは記録および再生のみといったように、扱われるA/Vデータに対する機能が限定されていた。したがって、このような、A/V機器において扱われるA/Vデータに対しては、記録媒体に記録されたA/Vデータに対して著作権に関する情報を付加することで、比較的容易に著作権の保護を行なう機構を実現することができた。
【0005】ところが、上述のようなA/Vデータファイルに対しては、このA/V機器において扱われるA/Vデータように、著作権の保護を行なう機構が導入されていなかった。そのため、このA/Vデータファイルの複写や加工が自由に行われてしまい、著作権の侵害が横行してしまうという問題点があった。
【0006】したがって、この発明の目的は、コンピュータ上で扱われるA/Vデータファイルに対して著作権情報を持たせ、この情報に基づきこのA/Vデータファイルの著作権を保護するようなファイル生成方法およびデータ処理方法を提供することにある。
【0007】
【課題を解決するための手段】この発明は、上述した課題を解決するために、ディジタルデータの著作権情報を第1の暗号化鍵に基づき暗号化する第1の暗号化ステップと、ディジタルデータをデータファイルのデータ部に格納し、暗号化した著作権情報をデータファイルの所定領域に格納してデータファイルを生成するステップとからなることを特徴とするファイル生成方法である。
【0008】また、この発明は、ディジタルデータと、暗号化されたディジタルデータの著作権情報とからなるデータファイルを受信するステップと、暗号化されたディジタルデータの著作権情報を復号化し、著作権情報を抽出するステップと、著作権情報に基づいて、ディジタルデータの取り扱いを制御するステップとからなることを特徴とするデータ処理方法である。

【0009】また、この発明は、第2の暗号化鍵で暗号化されたディジタルデータと、第1の暗号化鍵で暗号化されたディジタルデータの著作権情報及び第2の暗号化鍵とからなるデータファイルを受信するステップと、暗号化されたディジタルデータの著作権情報及び暗号化された第2の暗号化鍵を、第1の暗号化鍵で復号し、著作権情報及び第2の暗号化鍵を抽出するステップと、暗号化されたディジタルデータを、抽出した第2の暗号化鍵で復号するステップとからなることを特徴とするデータ処理方法である。

【0010】上述したように、請求項1に記載の発明は、ディジタルデータの著作権情報を第1の暗号化鍵に基づき暗号化し、ディジタルデータをデータファイルのデータ部に格納し、暗号化した著作権情報をデータファイルの所定領域に格納してデータファイルを生成するようにしているため、第1の暗号化鍵による暗号化を解かない限り、データファイルの所定領域に格納された著作権情報の不正な書き換えが防がれる。

【0011】また、請求項4に記載の発明は、ディジタルデータと、暗号化されたディジタルデータの著作権情報とからなるデータファイルを受信し、暗号化されたディジタルデータの著作権情報を復号化し、著作権情報を抽出して、著作権情報に基づいて、ディジタルデータの取り扱いを制御するようにしているため、著作権情報の暗号化を解かない限り、ディジタルデータを取り扱えないように制御することができる。

【0012】また、請求項6に記載の発明は、第2の暗号化鍵で暗号化されたディジタルデータと、第1の暗号化鍵で暗号化されたディジタルデータの著作権情報及び第2の暗号化鍵とからなるデータファイルを受信し、暗号化されたディジタルデータの著作権情報及び暗号化された第2の暗号化鍵を、第1の暗号化鍵で復号し、著作権情報及び第2の暗号化鍵を抽出して、暗号化されたディジタルデータを、抽出した第2の暗号化鍵で復号するようにしているため、第1の暗号化鍵を持っていなければ、ディジタルデータを復号できない。

【0013】

【発明の実施の形態】以下、この発明の実施の一形態について説明する。この発明では、コンピュータ上で扱われるA／Vデータファイルにおいて、属性（プロパティ）情報として著作権情報を持たせる。この著作権情報は、暗号化されて書き込まれるため、ユーザのエディタなどによる書き換えから保護される。この暗号化された著作権情報は、このA／Vデータファイルからデータが読み出される際に参照される。

【0014】図1は、以下の説明において想定するシステム構成を概略的に示す。ここでは、このように、所定のネットワーク2に対して、上述のA／Vデータファイル送出側のコンピュータ1とA／Vデータファイルを受け取る側のコンピュータ3a，3b，・・・とが接続されるシステムが想定される。なお、送出側のコンピュータ1も、受け取り側と同様に、複数接続されることができる。また、これらコンピュータ1および3a，3b，・・・は、所定のOS（Operation System）上で動作する。詳細は後述するが、このOSは、この実施の一形態における著作権保護システムに対応した機能を有する。

【0015】送出側のコンピュータ1で、所定のアプリケーションソフトウェアA（以下、ソフトウェアAと称する）で作成されたA／Vデータファイルがネットワーク2を介して受け取り側のコンピュータ3a，3b，・・・に受け取られる。そして、例えばコンピュータ3aにおいて、所定のアプリケーションソフトウェアB（以下、ソフトウェアBと称する）を用いてこのA／Vデータファイルが読み出される。なお、ソフトウェアAおよびソフトウェアBとは、同一のアプリケーションソフトウェアであってもよい。

【0016】上述の構成は一例であって、この発明は、例えばDVD（Digital Versatile Disk）－ROMドライブを内蔵したパーソナルコンピュータとディジタルVTRとが接続されたような場合にも適用することができる。

【0017】図2は、この実施の一形態におけるA／Vデータファイル構造の一例を概略的に示す。データは、全体的には一般的なファイル構造を有し、ヘッダ部，データ部，およびデリミタ部とからなる。

【0018】ヘッダ部は、このデータファイルの属性（プロパティ）情報が記される領域である。このプロパティ情報は、ソフトウェアやOSがこのファイルを識別するために必要な情報、例えばこのファイルのファイル名，ファイル形式，およびデータサイズなどの情報からなる。さらに、この一形態においては、このプロパティ情報に、暗号化された著作権情報が含まれる。OSやソフトウェアAあるいはBによってこの著作権情報が読み込まれ、この著作権情報に基づきこのファイルに対する著作権保護がなされる　著作権保護のための著作権情報がファイルのプロパティ情報として格納されるため、この著作権情報は、削除することができない。

【0019】データ部には、A／Vデータ本体、すなわち、音声データおよび／または画像データが格納される。このデータ部には、A／Vデータ本体に限らず、例えばプログラムやスクリプトなどを格納してもよい。また、これらA／Vデータおよびプログラムなどを混在させて格納することもできる。デリミタ部には、例えばこのファイルの終了情報が記される。

【0020】この発明においては、上述の著作権情報は、コピー世代の制限に関する制御情報（CGMS（Copy Generation Management System）と称する）およびアナログビデオ信号に対するコピー制限システムを指示する情報（APS（Analog Protection System）と称する）とからなる。この著作権情報には、これらの情報の他に

も、例えばこのA／Vデータファイルのデータ部に格納されるデータの著作者名，作成日などの、著作者がそのデータの著作権を主張するために必要な情報や、著作者の識別を行なう情報、例えば暗証番号やＩＤを含ませるようにしてもよい。

【００２１】ＣＧＭＳ情報およびＡＰＳ情報の一例を図３に示す。この図３Ａに示すように、ＣＧＭＳ情報は、２ビットのデータからなり、例えば下記のように定義される。

【００２２】００：コピー可能
０１：未使用
１０：コピー１世代可能
１１：コピー不可

【００２３】このA／Vデータファイルが係わるOSやソフトウェアによって、このCGMS情報が読み出され参照されることによって、このファイルを保存することが可能であるかどうかが判断される。

【００２４】図４は、ＣＧＭＳによるコピー世代制限のフローチャートを示す。ＣＧＭＳ情報を含むファイルを例えばコピーしようとした場合、先ず、ファイルのヘッダ部が読み込まれ、著作権情報に含まれるＣＧＭＳ情報が抽出される。そして、次のステップＳ２において、このＣＧＭＳ情報が上述の定義のうちのどの状態であるかが判断される。若し、ＣＧＭＳ情報が‘００’であれば、処理はステップＳ５に移行する。そして、ステップＳ５において、定義に従いこのファイルが保存可能であるとされ、コピーが行なわれファイルが保存される。

【００２５】また若し、ＣＧＭＳ情報がファイルのコピーを許可しない‘１１’であれば、処理はステップＳ３に移行し、定期に従いファイルが保存不可とされる。

【００２６】さらに若し、ＣＧＭＳ情報がファイルの１世代のみのコピーを許可する‘１０’であれば、処理はステップＳ４に移行する。ステップＳ４では、ＣＧＭＳ情報が‘１０’からファイルのコピーを許可しない‘１１’に変更される。ＣＧＭＳ情報が変更されると、処理はステップＳ５に移行し、コピーが行なわれ、ファイルが保存される。ＣＧＭＳ情報が‘１１’に変更されているため、このファイルはコピー不可とされ、これによりコピーの世代制限がなされる。

【００２７】なお、実際には、ファイルのコピーは、例えばファイルの内容が一旦バッファメモリなどに読み込まれ、メモリやディスクなどのデータ記憶媒体の別の領域に書き込まれることによってなされる。したがって、このファイルのコピーは、ファイルの保存と同等に扱うことができる。

【００２８】また、図３Ｂに示すように、ＡＰＳ情報は、上述のＣＧＭＳ情報と同様に２ビットのデータからなり、例えば下記のように定義される。

【００２９】００：ＡＰＳ　ＯＦＦ
０１：ＰＳＰ　ＯＮ，スプリットバーストＯＦＦ
１０：ＰＳＰ　ＯＮ，２ラインスプリットバーストＯＮ
１１：ＰＳＰ　ＯＮ，４ラインスプリットバーストＯＮ

【００３０】このＡＰＳ情報は、所定の方法で以てアナログビデオ信号に重畳されて、例えば外部のビデオテープレコーダやテレビジョンモニタに送出される。このＡＰＳ情報を受け取ったこれらの装置がこのＡＰＳに対応している場合、定義に従い発生されたアナログコピー制限用信号に基づいて生成されたコピー防止用信号によって、このビデオ信号の記録や映出を妨害することができる。

【００３１】ＡＰＳ　ＯＦＦでは、アナログコピー制限用信号を発生しない。ＰＳＰ　ＯＮは、疑似同期信号を含むコピー防止用信号を、アナログビデオ信号に対して重畳するシステムを動作させることを意味する。このシステムを動作させることで、このビデオ信号を供給されたビデオテープレコーダのＡＧＣを誤動作させ、正常な画像の記録を妨害することができる。

【００３２】また、スプリットバーストのＯＮは、その一部に反転バースト信号を挿入したカラーバースト信号を、アナログビデオ信号に対して付加するシステムを動作させることを意味する。このシステムを動作させることで、このビデオ信号を供給されたモニタやビデオテープレコーダなどで、ＡＰＣが正常な動作をすることができず、正常な画像の映出を妨害することができる。スプリットバーストとしては、２ライン単位で反転バースト信号を付加する２ラインスプリットバーストと、４ライン単位で反転バースト信号を付加する４ラインスプリットバーストとの二つの方式が用意され、その一方を選択的に動作させるようになされている。

【００３３】図５は、Ａ／Ｖデータファイルを保存する際の、ソフトウェアＡ，ＯＳ１１，およびＡ／Ｖデータファイル１２間における処理の推移を概略的に示す。Ａ／Ｖデータファイル１２は、例えば当初メモリ（図示しない）上に存在し、ソフトウェアＡに対してこのファイル１２の保存を指示することによって、このメモリからハードディスクなどの記録媒体（図示しない）に対して保存される。なお、これはこの例に限られず、例えばハードディスクの第１の領域から第２の領域へのＡ／Ｖデータファイルのコピー、あるいはネットワークを介して伝送されたＡ／Ｖデータの保存などにも適用できる。

【００３４】この例に示されるコンピュータにおいて、ソフトウェアによるメモリやハードディスクなどの各種デバイスに対するアクセスは、全てＯＳ１１を介してなされる。ソフトウェアＡに対して、作成されたＡ／Ｖデータファイル１２の保存が指示される。この指示は、所定の形式で以てソフトウェアＡからＯＳ１１に対して伝達される。そして、ソフトウェアＡが有する鍵ＫｃがＯＳ１１に対して渡される。すると、ＯＳ１１によって、先ず、メモリ上に存在するＡ／Ｖデータファイル１２の著作権情報が読み出される。換言するが、この著作権情

報は暗号化されているため、所定の方法で以て復号化される。

【００３５】解読された著作権情報からＣＧＭＳ情報が抽出され、上述の図４に示したフローチャートに従って、このＡ／Ｖデータファイル１２が保存可能であるかどうかが判断される。この判断の結果、保存可能であると判断されたら、このＡ／Ｖデータファイル１２がハードディスクの所定の領域に書き込まれ保存される。そして、ＯＳ１１によってこのファイル１２の書き込み確認がなされ、確認情報がソフトウェアＡに対して伝達され、この情報を受け取ったソフトウェアＡにおいて、ファイル１２の保存が正しく完了したとされる。

【００３６】ヘッダ部に含まれる著作権情報は、ユーザによって、例えばバイナリデータの編集が可能なエディタなどを用いて容易に書き換えられてしまうおそれがある。そこで、この発明においては、上述したように、この著作権情報を所定の方法で暗号化する。図６は、この著作権情報の暗号化の方法の一例を概略的に示す。例えば上述のソフトウェアＡでのＡ／Ｖデータの作成に伴い、著作権情報が作成される。この著作権情報には、例えば著作者名、データ作成日といった、このファイルに格納されるＡ／Ｖデータの著作権を主張するために必要な情報と、上述のＣＧＭＳ情報とが含まれる。

【００３７】この著作権情報が例えば所定の文字列からなる暗号化鍵ｋｃに基づき暗号化される。暗号化鍵ｋｃは、特定のソフトウェアに依存するもので、例えば、上述のＡ／Ｖデータファイルを作成するソフトウェアＡや、作成されたファイルを読み込み再生あるいは実行するソフトウェアＢに対して入力されたユーザのパスワードＰｗに基づいて生成される。また、これらのソフトウェアが予めこの鍵ｋｃを有しているとしてもよい。

【００３８】この鍵ｋｃによる暗号化の例として、例えば鍵ｋｃに基づく所定の方法で以て、著作権情報を構成する記号あるいは文字列に対して転字や換字を繰り返し行なう方法が挙げられる。暗号化された著作権情報がヘッダ部にプロパティ情報として格納されると共に、作成されたＡ／Ｖデータが所定の領域に格納され、Ａ／Ｖデータファイルが作成される。

【００３９】このＡ／Ｖデータファイルに含まれる、暗号化された著作権情報は、図７に概略的に示されるように、鍵ｋｃで以て暗号化のときとは逆の手順で復号化される。すなわち、例えばソフトウェアＢにおいて、Ａ／Ｖデータファイルのヘッダ部に格納されたプロパティ情報が読み出され、このプロパティ情報に含まれる暗号化された著作権情報が抽出される。そして、ソフトウェアＢが予め有している鍵ｋｃが用いられ、鍵ｋｃに基づき所定の方法で以て暗号化された著作権情報が復号化される。上述の、ＣＧＭＳによるコピー世代制限は、この復号化された著作権情報に対してなされる。

【００４０】なお、これら図６および図７に示した著作権情報の暗号化／復号化の手順は、原理的なものであり、この実施の一形態に適用されるに止まらず、後述する変形例にも適用されるものである。

【００４１】図８は、上述の図６および図７に示した著作権情報の暗号化および復号化の手順を、この実施の一形態に適合させより具体的に示す。この例では、著作権情報を暗号化する際の暗号化鍵ｋｃは、ＯＳ１１において、ユーザパスワードＰｗおよびマスタ鍵ｋｍとに基づき生成される。

【００４２】ユーザパスワードＰｗは、例えば、ユーザによって指定される所定の文字列からなり、ＯＳ１１において、ログインするユーザに対して個別に設定される。また、このパスワードＰｗは、ソフトウェアＡにおいて設定されるようにしてもよい。パスワードＰｗは、ＯＳ１１において設定された場合には、ＯＳ１１の起動毎、ソフトウェアＡにおいて設定された場合には、ソフトウェアＡの起動毎に、ユーザに対して入力が求められる。マスタ鍵ｋｍは、所定の文字列からなり、例えばＯＳ１１のコンピュータ１に対するインストールの際になされるユーザ登録によって設定される。

【００４３】ＯＳ１１によって、Ａ／Ｖデータファイル１２のヘッダ部のプロパティ情報から暗号化された著作権情報が読み出される。この著作権情報は、ＯＳ１１において、上述の鍵ｋｃに基づき復号化される。そして、復号化された著作権情報からＣＧＭＳ情報が抽出され、このＣＧＭＳ情報に基づきこのファイル１２の保存の禁止／許可が判断される。

【００４４】この場合、復号化された著作権情報に基づきこのファイル１２に対するアクセスそのものの禁止／許可を判断するようにもできる。これは、例えば、パスワードＰｗがソフトウェアＡに対して設定された場合に、この著作権情報がソフトウェアＡに渡され、ソフトウェアＡにおいてパスワードＰｗとこの著作権情報とが照合され、その結果がＯＳ１１に渡されることによってなされる。

【００４５】一方、ソフトウェアＡにおいて作成されたＡ／Ｖデータに対してＣＧＭＳ情報が設定され、Ａ／Ｖデータファイルとして保存される際に、ＯＳ１１において、鍵ｋｃに基づいて著作権情報の暗号化がなされる。

【００４６】この実施の一形態では、Ａ／Ｖデータファイルの著作権保護のためのＣＧＭＳ情報の、例えば照合や書き換えといった処理は、ＯＳ１１においてなされる。このＯＳ１１上では、作成される全てのファイルに対して著作権情報が設定され、全てのファイル操作の際に、この設定された著作権情報の照合などの処理がなされる。そこで、この著作権保護システムに対応していない、他のＯＳ上で作成されたファイル操作に対して互換性を持たせる必要がある。

【００４７】図９は、このファイルの互換性を考慮した、ＯＳ１１におけるファイルに対するアクセスのフロ

ーチャートを示す。ファイルに対するアクセスがなされると、先ず、ステップＳ１０において、このファイルがＯＳ１１による著作権保護システムに対応しているかどうかが判断される。この判断は、例えば、ＯＳ１１において著作権保護システムに対応しているファイルにはヘッダ部にその旨を示すフラグなどを記し、このフラグの有無を調べることによって行なうことができる。また、ヘッダ部の著作権情報そのものの有無を調べるようにしてもよい。

【００４８】若し、著作権保護システムに対応していないと判断されたら、このファイルに対する著作権保護の手段はとられず、ステップＳ１７においてファイルの保存がなされる。

【００４９】一方、ステップＳ１０でファイルが著作権保護システムに対応していると判断されたら、処理はステップＳ１１に移行する。そして、ステップＳ１１において、このファイルの著作権情報が読み出され、復号化される。この復号化は、例えばＯＳ１１から所定のソフトウェア（例えば上述のソフトウェアＡあるいはＢ）に対して暗号化鍵ｋｃを要求し、この要求に対してそのソフトウェアから渡された鍵ｋｃに基づいてなされる。著作権情報の復号化がなされると、処理はステップＳ１２に移行する。

【００５０】ステップＳ１２では、復号化された著作権情報からＣＧＭＳ情報が抽出される。そして、次のステップＳ１３で、ＣＧＭＳ情報の状態が判断される。若し、ＣＧＭＳ＝’１１’であれば、処理はステップＳ１４に移行し、上述のＣＧＭＳの定義に従いファイル保存は不可であるとされる。また若し、ＣＧＭＳ＝’００’であれば、定義に従いファイル保存が可能とされるため、処理はステップＳ１６に移行する。さらに若し、ＣＧＭＳ＝’１０’であれば、処理はステップＳ１５に移行し、ＣＧＭＳ情報が’１１’に書き換えられる。そして、処理は次のステップＳ１６に移行する。

【００５１】ステップＳ１６において、著作権情報が暗号化される。この暗号化は、例えばＯＳ１１から所定のソフトウェアに対して暗号化鍵ｋｃを要求し、この要求に対してそのソフトウェアから渡された鍵ｋｃに基づいてなされる。暗号化がなされると、ファイルのヘッダ部に含まれる著作権情報がこのステップＳ１６で暗号化された著作権情報とされる。そして、次のステップＳ１７で、このファイルが保存される。

【００５２】なお、上述の説明では、ネットワーク２に接続されたコンピュータ１および３ａ，３ｂ，・・・のそれぞれには、全て同一のＯＳ１１が搭載されているとしたが、これはこの例に限定されない。コンピュータ１および３ａ，３ｂ，・・・に対してそれぞれ異なるＯＳが搭載されている場合でも、互いに共通のプロトコルで以てデータ通信を行なうことができれば、この発明による著作権保護システムを適用することができる。

【００５３】また、上述のフローチャートは、著作権保護システムに対応していないファイルの互換性が考慮されたものだが、この処理を応用することによって、著作権保護を必要とされないファイルを選択的に設定することができる。

【００５４】Ａ／Ｖデータファイルは、データファイルとしてのコピーが行なわれるだけでなく、例えばコンピュータによってこのファイルが再生あるいは実行され、アナログ方式やディジタル方式のビデオ信号とされ外部に出力されることも考えられる。この出力されたビデオ信号は、例えばアナログビデオテープレコーダによって記録され、それによりＡ／Ｖデータに対する著作権の侵害が生じる可能性がある。したがって、このような場合における著作権保護についても考慮する必要がある。

【００５５】図１０は、Ａ／Ｖデータファイルから再生されたＡ／Ｖデータがコンピュータ外部に対して出力される場合の、データ変換の方法を概念的に示す。ここでは、Ａ／Ｖデータがアナログ３原色信号に変換され出力される例を示す。図示せずとも、ソフトウェアＡによってＡ／Ｖデータファイル１２が再生され、Ａ／Ｖデータが出力される。このＡ／Ｖデータは、エンコーダ２０に供給され、Ｄ／Ａ変換されると共に、例えばＲＧＢの各色の信号からなるコンポーネントビデオ信号とされる。このコンポーネントビデオ信号のうち、例えばＲ信号が加算器２２の一方の入力端に対して供給される。

【００５６】この加算器２２は、他方の入力端に供給された信号の、一方の入力端に供給されたビデオ信号に対する加算を、ヒデオ信号に同期して所定のタイミングで以て制御することができる。これは、例えばエンコーダ２０において、Ａ／Ｖデータをビデオ信号に変換する際に用いられたタイミング信号に基づき生成された制御信号が、この加算器２２に供給されることによってなされる。

【００５７】一方、ソフトウェアＡあるいはＯＳ１１によって、Ａ／Ｖデータファイルから著作権情報が読み出される。この著作権情報が鍵ｋｃによって復号化され、ＡＰＳ情報が抽出される。そして、このＡＰＳ情報に基づきアナログコピー制限用信号が生成され、生成されたこの信号は、加算器２２の他方の入力端に供給される。加算器２２では、この信号を、一方の入力端に供給されているＲ信号の、例えば垂直ブランキング期間に加算する。

【００５８】図示しないが、このアナログビデオ信号は、モニタに対して供給され映出されると共に、例えばＡＰＳに対応したＲＧＢ信号／コンポジットビデオ信号変換器に供給される。コピー制限用信号は、ブランキング期間に重畳されているため、モニタへの映出には直接的な影響はない。しかしながら、ＡＰＳに対応したＲＧＢ信号／コンポジットビデオ信号変換器を介して外部にコンポジットビデオ信号として出力された場合、上述の

図３Ｂに一例が示される、ＡＰＳ情報の定義に基づいたコピー防止用信号がこのビデオ信号に対して重畳または付加される。そのため、このビデオ信号をビデオテープなどに記録しても、正常な画像として再生することができず、結果的にＡ／Ｖデータに対する著作権を保護することができる。

【００５９】なお、Ａ／Ｖデータファイルが再生されディジタル画像データとして外部に出力される場合には、著作権情報から抽出されたＣＧＭＳ情報およびＡＰＳ情報とがそのまま伝送され、例えばディジタルビデオカセットレコーダによって、テープの所定の領域に記録される。したがって、この場合でも容易にコピー防止の効果を得ることができる。

【００６０】次に、この発明の実施の一形態の変形例について説明する。図１１は、この変形例におけるＡ／Ｖデータファイル構造の一例を概略的に示す。この変形例においては、データ部に格納されたＡ／Ｖデータが所定の暗号化鍵ｋｄに基づき暗号化され、この鍵ｋｄがＡ／Ｖデータファイルのヘッダ部の著作権情報と共に、所定の暗号化鍵に基づき暗号化される。この変形例では、このようにＡ／Ｖデータそのものを暗号化することにより、より強固にＡ／Ｖデータの著作権保護を行なうものである。

【００６１】図１２は、この変形例によるＡ／Ｖデータファイルの暗号化の方法の一例を概略的に示す。この例においては、Ａ／Ｖデータファイル供給側からユーザに対して配布される顧客管理鍵ｋｕを用いて、著作権情報およびデータ暗号化鍵ｋｄの暗号化を行なう。

【００６２】Ａ／Ｖデータは、このデータの供給側で管理しているデータ暗号化鍵ｋｄに基づいて暗号化される。この暗号化には、例えば、鍵ｋｄに基づいた所定の規則に従って転字や換字を繰り返すことによってなされる。この暗号化されたＡ／Ｖデータは、Ａ／Ｖデータファイルのデータ部に格納される。また、このＡ／Ｖデータの暗号化に用いられた鍵ｋｄは、著作権情報と共に、Ａ／Ｖデータの供給側において管理される顧客管理鍵ｋｕに基づき暗号化される。この顧客管理鍵ｋｕは、例えばこのＡ／Ｖデータの供給を受けた顧客のそれぞれに対して設定され、Ａ／Ｖデータ供給側から渡される。こうして暗号化された著作権情報および鍵ｋｄとは、プロパティ情報としてＡ／Ｖデータファイルのヘッダ部に格納される。

【００６３】図１３は、この変形例によるＡ／Ｖデータファイルの復号化の方法の一例を概略的に示す。Ａ／Ｖデータの供給側からユーザに対して渡されたＡ／Ｖデータファイルにおいて、ヘッダ部が読み込まれ、暗号化された著作権情報およびデータ暗号化鍵ｋｄが抽出される。また、Ａ／Ｖデータ供給側からユーザに対して、予め顧客管理鍵ｋｕが渡される。ヘッダ部から抽出された暗号化された著作権情報および鍵ｋｄがこの顧客管理鍵ｋｕによって復号化される。そして、この復号化された顧客管理鍵ｋｕによって、データ部に格納された、暗号化されたＡ／Ｖデータが復号化される。

【００６４】この例のように、顧客管理鍵ｋｕを用いることによって、Ａ／Ｖデータ供給側は、ユーザに対してＡ／Ｖデータファイルの使用を限定することができ、Ａ／Ｖデータ供給側における顧客管理を行なうことができる。そのため、この顧客管理鍵ｋｕを用いた方法は、例えば大量生産されるＡ／Ｖデータファイルに対して用いて好適なものである。

【００６５】一方、上述の実施の一形態における著作権保護の方法は、例えば個人の創作に関する著作権の保護に対して用いて好適である。

【００６６】なお、この変形例は、この例に限らず、例えば顧客管理鍵ｋｕの代わりに、上述の実施の一形態において用いられた暗号化鍵ｋｃを用いることも可能である。勿論この場合には、Ａ／Ｖデータ供給側による顧客管理は、厳密には行なわれない。

【００６７】上述の実施の一形態およびその変形例とにおいては、著作権情報処理に対応したＯＳに対してこの発明が適用されるように説明したが、これは、この例に限定されるものではない。図１４は、この発明の別の変形例として、著作権情報処理に対応していないＯＳに対してこの発明が適用された際の、ソフトウェアＡ’、ＯＳ１１’、Ａ／Ｖデータファイル１２間における処理の推移を概略的に示す。なお、この別の変形例は、上述の実施の一形態およびその変形例とにより何方のファイル構造に対しても適用可能なものである。

【００６８】この別の変形例においては、上述の実施の一形態およびその変形例ではＯＳ１１においてなされていた、Ａ／Ｖデータファイルからの著作権情報の読み出しおよび読み出された著作権情報の解読を、ソフトウェアＡ’上で行なう。Ａ／Ｖデータファイル１２は、当初図示されないメモリ上に存在し、ソフトウェアＡ’に対してこのファイル１２の保存を指示することによって、このメモリから例えば図示されないハードディスクに対して保存される。なお、これはこの例に限られず、例えばハードディスクの第１の領域から第２の領域へのＡ／Ｖデータファイルのコピー、あるいはネットワークを介して伝送されたＡ／Ｖデータの保存などにも適用できる。

【００６９】ソフトウェアＡ’に対して、作成されたＡ／Ｖデータファイル１２の保存が指示される。この指示に基づき、Ａ／Ｖデータファイル１２のヘッダ部からプロパティ情報が読み出され、読み出されたこのプロパティ情報から著作権情報が抽出される。この著作権情報は、例えばソフトウェアＡ’が固有に有している暗号化鍵ｋｃによって暗号化されている。この鍵ｋｃに基づき著作権情報が復号化され、解読される。

【００７０】なお、著作権情報の暗号化に用いられた暗

号化鍵は、この例のような暗号化鍵ｋｃに限られない。例えば、上述の、Ａ／Ｖデータファイル供給側からユーザに対して渡された顧客管理鍵ｋｕをこの暗号化鍵として用いるようにもできる。

【００７１】解読された著作権情報からＣＧＭＳ情報が抽出され、上述の図４に示したフローチャートに従って、このＡ／Ｖデータファイル１２が保存可能であるかどうかが判断される。この判断の結果、保存可能であると判断されたら、ＯＳ１１'によって、このＡ／Ｖデータファイル１２が例えばハードディスクの所定の領域に書き込まれ保存される。そして、ＯＳ１１'によってこのファイル１２の書き込み確認がなされ、確認情報がソフトウェアＡ'に対して伝達され、この情報を受け取ったソフトウェアＡ'において、ファイル１２の保存が正しく完了したとされる。

【００７２】

【発明の効果】以上説明したように、この発明によれば、Ａ／Ｖデータファイルのプロパティ情報に、著作権保護を行なうための著作権情報が含まれる。そのため、コンピュータ上で扱われるＡ／Ｖデータに対しても、著作権保護の機構を導入することができ、著作権の侵害が防止される効果がある。

【００７３】また、この発明によれば、著作権情報に対してコピーの世代制限を制御するＣＧＭＳ情報が含まれ、ディジタルＡ／Ｖ機器などで既に導入されているものと同一の概念でＡ／Ｖデータの著作権保護が行なわれる。そのため、コンピュータ上のＡ／Ｖデータとディジタル Ａ／Ｖ機器との間で、著作権保護の考え方に整合性がとれる効果がある。

【００７４】さらに、この発明によれば、著作権情報は、暗号化されているため、ユーザによる不正な書き換えなどから保護され、安全性が高いという効果がある。

【００７５】さらにまた、この発明によれば、ＯＳにおいてファイルの更新や保存の際に著作権情報が含まれるプロパティ情報を参照するようにされているため、アプリケーションソフトウェアだけで同様の処理を行なう場合に比べ、著作権保護の確実性がより高まるという効果がある。

【００７６】また、この発明による著作権保護のための処理は、高々数バイトのデータをソフトウェアあるいはＯＳ上でハンドリングするだけで行なわれるので、著作権保護のために新たに発生するコストは無視できる程度のものであるという効果がある。

【００７７】さらに、この発明による著作権情報は、Ａ／Ｖデータファイルのプロパティ情報として扱われるため、ファイルから削除することができず、より確実に著作権保護を行なうことができるという効果がある。

【００７８】また、この発明による著作権情報は、既に存在するディジタルＡ／Ｖ機器における著作権保護と共通の考えに基づいて設定されている。そのため、この発明によるＡ／Ｖデータは、ディジタルＡ／Ｖ機器とのインターフェイス上にそのまま伝送することができるという効果がある。

【図面の簡単な説明】

【図１】説明において想定されるシステム構成を概略的に示す図である。

【図２】実施の一形態におけるＡ／Ｖデータファイル構造の一例を概略的に示す図である。

【図３】ＣＧＭＳ情報およびＡＰＳ情報の一例を示す略線図である。

【図４】ＣＧＭＳによるコピー世代制限のフローチャートである。

【図５】Ａ／Ｖデータファイルを保存する際の、ソフトウェア，ＯＳ，およびＡ／Ｖデータファイル間における処理の推移を概略的に示す図である。

【図６】著作権情報の暗号化の方法の一例を概略的に示す図である。

【図７】著作権情報の復号化の一例を概略的に示す図である。

【図８】著作権情報の暗号化および復号化の手順をより具体的に示す図である。

【図９】ファイルの互換性を考慮した、ＯＳにおけるファイルに対するアクセスのフローチャートである。

【図１０】Ａ／Ｖデータファイルを外部出力する場合のデータ変換の方法を概念的に示す図である。

【図１１】変形例におけるＡ／Ｖデータファイル構造の一例を概略的に示す図である。

【図１２】顧客管理鍵ｋｕを用いた場合の、Ａ／Ｖデータファイルの暗号化の方法の一例を概略的に示す図である。

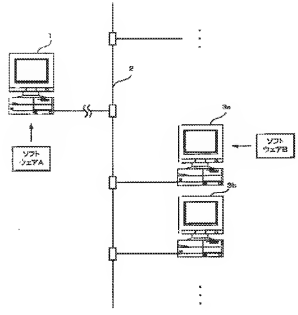
【図１３】顧客管理鍵ｋｕを用いた場合の、Ａ／Ｖデータファイルの復号化の方法の一例を概略的に示す図である。

【図１４】ＯＳが著作権情報処理に対応していない場合の、ソフトウェア，ＯＳ，Ａ／Ｖデータファイル間における処理の推移を概略的に示す

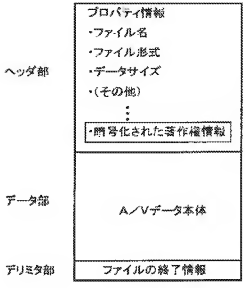
【符号の説明】

１，３ａ，３ｂ・・・コンピュータ、１１・・・ＯＳ、１２・・・Ａ／Ｖデータファイル、Ａ，Ｂ・・・アプリケーションソフトウェア、ｋｃ・・・暗号化鍵、ｋｄ・・・データ暗号化鍵、ｋｍ・・・マスク鍵、ｋｕ・・・顧客管理鍵、Ｐｗ・・・ユーザパスワード

【図1】




【図2】




【図3】

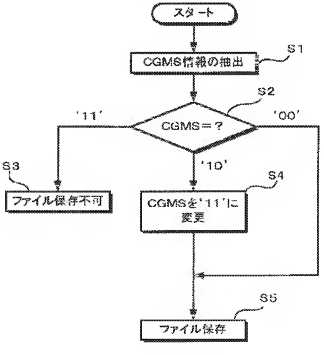
A

| CGMS | | 定義 |
|---|---|---|
| 1 | 1 | コピー不可 |
| 1 | 0 | コピー1世代可能 |
| 0 | 1 | 未使用 |
| 0 | 0 | コピー可能 |

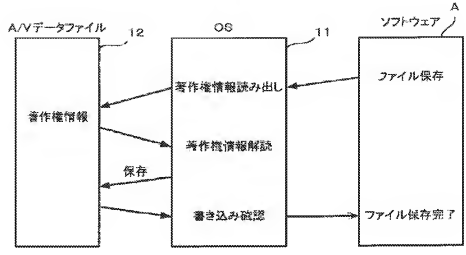
B

| フラグ | | 定義 |
|---|---|---|
| 0 | 0 | OFF |
| 0 | 1 | HSP ON |
| 1 | 0 | PSP ON, 2ラインスプリットバーストON |
| 1 | 1 | PSP ON, 4ラインスプリットバーストON |

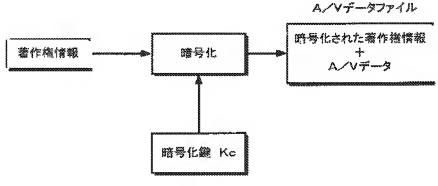
【図4】



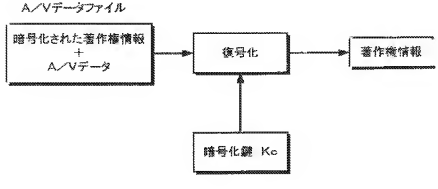
【図5】


A/Vデータファイル
12
OS
11
ソフトウェア
A
著作権情報
著作権情報読み出し
ファイル保存
著作権情報解読
保存
書き込み確認
ファイル保存完了

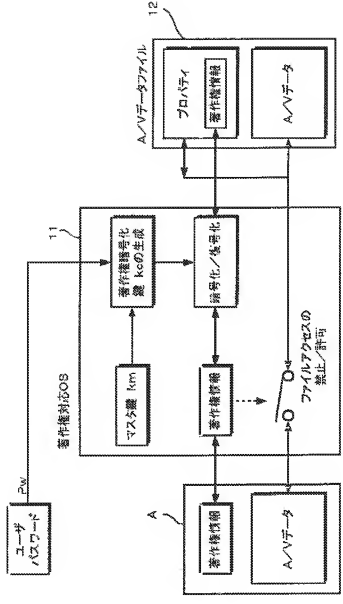
【図6】


A/Vデータファイル
著作権情報
暗号化
暗号化された著作権情報
+
A/Vデータ
暗号化鍵 Kc

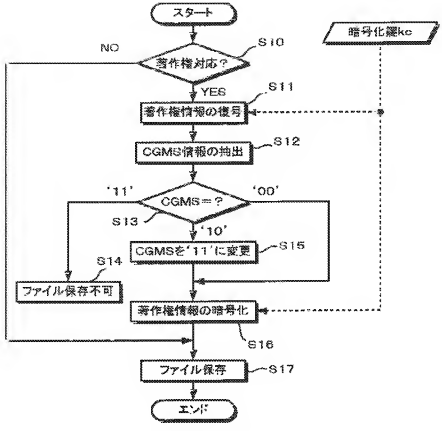
【図7】


A/Vデータファイル
暗号化された著作権情報
+
A/Vデータ
復号化
著作権情報
暗号化鍵 Kc

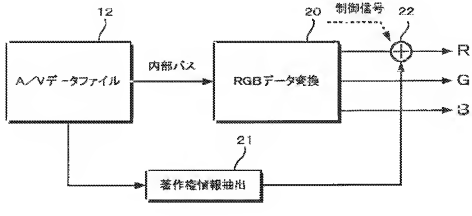
【図8】


12
A/Vデータファイル
プロパティ
著作権情報
A/Vデータ
11
著作権対応OS
著作権暗号化鍵 Kcの生成
マスク鍵 Km
著作権管理
暗号化／復号化
ファイルアクセスの禁止／許可
A
著作権情報
A/Vデータ
Pw
ユーザパスワード

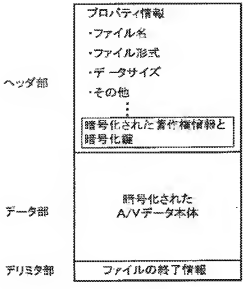
【図9】


スタート
暗号化鍵kc
NO
S10
著作権対応？
YES
S11
著作権情報の復号
S12
CGMS情報の抽出
'11'
CGMS＝？
'00'
S13
'10'
CGMSを'11'に変更
S15
S14
ファイル保存不可
著作権情報の暗号化
S16
ファイル保存
S17
エンド

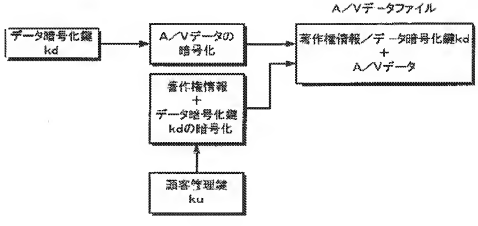
【図10】


12
A／Vデータファイル
内部バス
20
制御信号
22
RGBデータ変換
R
G
B
21
著作権情報抽出

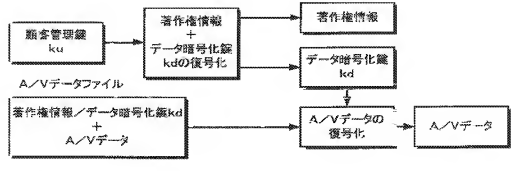
【図11】


プロパティ情報
・ファイル名
・ファイル形式
・データサイズ
・その他
暗号化された著作権情報と暗号化鍵
ヘッダ部
暗号化された
A/Vデータ本体
データ部
ファイルの終了情報
デリミタ部

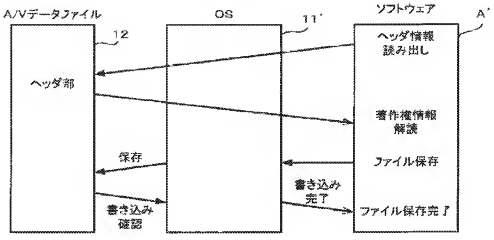
【図12】


A/Vデータファイル
データ暗号化鍵
kd
A/Vデータの
暗号化
著作権情報/データ暗号化鍵kd
+
A/Vデータ
著作権情報
+
データ暗号化鍵
kdの暗号化
顧客管理鍵
ku

【図13】


顧客管理鍵
ku
著作権情報
+
データ暗号化鍵
kdの復号化
著作権情報
データ暗号化鍵
kd
A/Vデータファイル
著作権情報/データ暗号化鍵kd
+
A/Vデータ
A/Vデータの
復号化
A/Vデータ

【図14】




フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | FI | | (参考) |
|---|---|---|---|---|
| H04L 9/32 | | H04L 9/00 | 601A | |
| H04N 5/91 | | | 671 | |

Fターム(参考) 5B017 AA03 BA07 CA09 CA16
5B082 EA11 GA11
5C053 FA13 FA24 GB06 JA21 LA11
5D044 AB05 AB07 BC02 CC04 DE49
DE50 DE53 EF05 FG18 GK17
HL08
5J104 AA15 AA16 EA17